

CDI Information Security Policy

To: CDI Employees

No.: ISO-07

From: Information Security Office (ISO)

Issued: August 1, 2004

Subject: Software and Freeware Policy

Expires: When Superseded

Policy

It is the policy of the California Department of Insurance (CDI) that all licensed software and freeware (i.e., licensed without cost) that is purchased, acquired, used, installed, or downloaded on CDI computers must be authorized by the Information Technology Division (ITD). The use of such software must comply with the computer software's licensing agreement and comply with copyright laws protecting the computer software.

To ensure state funds are not used to acquire, operate or maintain computer software in a manner that does not comply with applicable copyright laws, all CDI software contracts will use the language developed by the Department of General Services (DGS) Management Memo 00-02. DGS requires certification that appropriate systems and controls are in place to prevent state funds from being used on anything other than officially licensed software.

If there is a CDI business need to use non-licensed or unauthorized software, the employee must request approval from ITD to use the software on CDI equipment by submitting an [IT Procurement Request \(ITPR\) - ITD 005](#). The request must clearly state the business need and show evidence that installation of the software will not violate its license agreement.

Furthermore, employees may not install any software on CDI equipment without prior approval of ITD. Software must be installed on CDI computers in compliance with the computer software's licensing agreement. Employees may not install non-licensed and/or unauthorized software on CDI equipment. The computer software must be on the CDI software standards list and must be approved by ITD.

Installation and removal of software from CDI equipment must be by, or under the supervision of the ITD help desk staff. When the non-CDI owned and licensed software is no longer needed for CDI business, the employee's supervisor or manager must advise the employee to have the software removed by ITD help desk staff from CDI equipment.

Purpose

The purpose of this policy is to ensure that only approved and licensed software are run on CDI systems and to reduce ITD help desk calls for unsupported software. This procedure ensures that only authorized software is being used on CDI networks, systems, desktops, laptops or other electronic devices. The policy also protects the department from any legal liability for non-licensed software.

“At-Risk” Software

It is the policy of CDI to prohibit the use of software on CDI networks, systems, desktops, laptops or other electronic devices that pose a risk to the networks or systems and/or the information stored on them. ITD staff will monitor CDI’s networks, systems and any connecting devices to determine if “at-risk” software is being used.

Examples of “at-risk” software are any hacking software, remote control software, peer-to-peer software (i.e. Kazaa, Instant Messenger programs), forensic, or auditing software. Any non-licensed or non-CDI approved software is considered “at-risk” software. If you have any questions regarding this policy please contact ISO.

Procedure

Managers and supervisors are responsible for ensuring that their employees are informed of this policy at the time of hiring. In addition, employees are to be reminded of the policy on a biennial basis.

Inquiries

Please contact the ISO at 916-492-3256 or 916-492-3353 if you have any questions regarding this policy.

Archie Alimagno, Information Security Officer